IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

K.MIZRA LLC, Plaintiff, v. SONICWALL INC., Defendant.	Civil Action No.: _____ **Jury Trial Demanded**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint for patent infringement against Defendant SonicWall Inc. ("SonicWall"), alleging as follows:

I. INTRODUCTION

1. K.Mizra is a patent licensing company run by experienced management. The company focuses on high value, high quality patents with a global reach. It owns patent portfolios originating with a wide array of inventors, including portfolios developed by well-known multinationals such as IBM, Intel, Rambus and others, as well as from research institutes such as Nederlandse Organisatie voor Toegespast Natuurwetenschappelijk Onderzoek (Netherlands Organization for Applied Scientific Research). By focusing on high quality patents, K.Mizra provides a secondary market for inventors to recoup their research and development investments and to continue their innovations. K.Mizra offers licenses to its patents on reasonable terms and in this way plays an important part in the development of the technologies that improve all our lives.

2. K.Mizra is the owner by assignment of United States Patent Nos. 8,234,705 ("the '705 Patent") and 9,516,048 ("the '048 Patent" and collectively with the '705 Patent, "the Asserted Patents"). The Asserted Patents were involved in unsuccessful *Inter Partes* Review Proceedings

("IPRs") and several now-resolved federal court litigations, and were originally invented by two highly respected and prolific individual inventors, James A. Roskind and Aaron T. Emigh.

3. The Asserted Patents were originally owned by Dr. Roskind and Mr. Emigh's company, Radix Labs, LLC. Dr. Roskind and Mr. Emigh were then, and remain today, focused on innovation, conducting new research, developing new technologies, and creating new and innovative computer products.

4. Dr. Roskind, one of the two inventors of the Asserted Patents, has bachelor's, master's, and doctorate degrees from MIT in both electrical engineering and computer science, and is the named inventor of over 300 U.S. patents. He has worked for Netscape as the Chief Architect and as the Netcenter Security Architect and was a co-founder for Infoseek, a company that was eventually acquired by Disney for $770 million. He was also a key developer of Google's "transport protocol" that provides the tech giant billions of dollars in value every year.

5. Mr. Emigh, the other named inventor of the Asserted Patents, graduated from the University of California, Santa Cruz with degrees in linguistics and computer and information sciences, and is the named inventor of over 140 patents. Prior to working with Dr. Roskind, Mr. Emigh worked in various positions developing software, including working as a software manager, architect, and engineer for Unicom and working as a manager for the software development and technical marketing groups for Philips TriMedia. He has founded or co-founded many companies, in addition to Radix Labs, LLC, including CommerceFlow, Inc., which was acquired by eBay for its technology that Mr. Emigh helped to develop.

6. After the Asserted Patents issued, Dr. Roskind and Mr. Emigh recouped their research and development investment by selling their rights thereto and continued on in their individual technology development pursuits. K.Mizra ultimately acquired the Asserted Patents and

licensed them to many of the who's-who of the tech world. Some of the accused infringers chose to test the validity of the Asserted Patents prior to settling their lawsuits involving the Asserted Patents. For instance, a few accused infringers of the Asserted Patents previously sought IPR by the Patent Trial and Appeal Board ("PTAB") of each of the Asserted Patents. A Final Written Decision ("Decision") in the '705 Patent IPR found that the petitioners had not shown, by a preponderance of the evidence, that the asserted claims were unpatentable. Based on the '705 Patent IPR Decision, the similar '048 Patent IPR was not even instituted. The '705 Patent IPR Decision was appealed to the Court of Appeals for the Federal Circuit ("CAFC"), resulting in a procedurally focused remand back to the PTAB. Prior to the issuance of the mandate that would have sent the '705 Patent IPR back to the United States Patent and Trademark Office ("USPTO") for further consideration, the parties agreed to move to dismiss the appeal.

7. K.Mizra remains ready, willing, and able to provide commercially-reasonable licenses for its various patented technologies to all entities who wish or need to use them internally or in connection with products or services offered to others. As outlined below, SonicWall is one such entity.

II. THE PARTIES

8. K.Mizra is a Delaware limited liability company with a mailing address of 777 Brickell Avenue, #500-96031, Miami, Florida 33131, and operates in Florida. K.Mizra is the owner by assignment of the Asserted Patents.

9. SonicWall is a corporation organized and existing under the laws of the state of Delaware with a principal place of business at 1033 McCarthy Boulevard, Milpitas, California 95035. *See* https://www.sonicwall.com/customers/contact-sales (last accessed Jan. 6, 2025), a true

and correct copy of which is attached as Ex. 1. This exhibit, and all other exhibits referenced in this Complaint, are incorporated by reference in their entireties.

10. SonicWall may be served through its registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

III. JURISDICTION AND VENUE

11. This is an action for patent infringement under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*, including 35 U.S.C. §§ 271, 281, and 284, among others. The Court has subject-matter jurisdiction over the claims raised in this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over SonicWall by virtue of, *inter alia*, its incorporation in Delaware, its appointment of a registered agent in Delaware, its conduct of business in this District, its purposeful availment of the rights and benefits of Delaware law, and its substantial, continuous, and systematic contacts with the state of Delaware and this District. SonicWall: (1) intentionally markets and sells its infringing products directly and through agents to residents of Delaware; (2) enjoys substantial income from the state of Delaware; and/or (3) directly, by its own actions, and/or in combination with actions of customers and others under its control, has committed acts of infringement in this District at least by making and using infringing systems and using, selling, and offering for sale infringing services.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1400(b) because SonicWall is incorporated in the state of Delaware and thus is a resident of the state.

IV. GENERAL ALLEGATIONS

A. The Asserted Patents

14. K.Mizra is the sole owner by assignment of the Asserted Patents with the full and exclusive right to bring suit to enforce them. (*See* Exhibit 2.) K.Mizra is also entitled to sue to collect damages for all past infringement of the Asserted Patents.

15. The ’705 Patent, titled “Contagion Isolation and Inoculation,” was legally issued by the USPTO to Inventors Roskind and Emigh on July 31, 2012. A true and correct copy of the ’705 Patent is attached hereto as Exhibit 3.

16. The ’048 Patent, titled “Contagion Isolation and Inoculation Via Quarantine,” and was issued by the USPTO to inventors Emigh and Roskind on December 6, 2016. A true and correct copy of the ’048 Patent is attached hereto as Exhibit 4.

17. The Asserted Patents share similar (and in some respects, identical) specifications and claims, with both claiming priority to U.S. Provisional Application No. 60/613,909, filed on September 27, 2004 (the “Provisional Application”).

B. Prior Licensing and Litigation of the Asserted Patents

18. The Asserted Patents have been owned by several entities, in addition to Radix and K.Mizra, with some of those entities issuing to third parties certain rights to the technologies covered thereby.

19. K.Mizra has been involved in a number of actions it was required to institute to protect its patent rights, including actions involving the Asserted Patents. Most of those actions resulted in the execution of confidential patent license agreements.

20. SonicWall is not and has never been a licensee of the Asserted Patents nor had or has any rights to use technologies covered by the Asserted Patents. SonicWall thus has no ownership or other rights (and is entitled to no rights) relating to the Asserted Patents.

C. Computer network Security Problems in 2004 Solved by the Asserted Patents

21. The technology described in the Asserted Patents was invented by Dr. Roskind and Mr. Emigh, two colleagues living in the same area who had similar interests in innovating computer-related technologies. In 2003, the inventors decided to create a business—Radix Labs, LLC—which focused on developing intellectual property related to various computer technologies, including computer network security technologies. The inventors focused on conceiving and reducing to practice inventions that they knew were needed (or soon would be needed) in the computer networking industry and then on drafting patent applications to capture and protect their technological innovations. In September of 2004, the inventors filed the Provisional Application to which both Asserted Patents claim priority. The Provisional Application described technology that focused on securing a computer network against the threats to which it was exposed when computer endpoints (e.g., laptop computers) were connected to a computer network. The Provisional Application, and by natural extension the Asserted Patents, also focus on remedying identified threats and quarantining those threats to mitigate any damage to the secured network.

22. Claims of the Asserted Patents are directed to technological solutions that address specific challenges grounded in computer network security. Maintaining the security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, data corruption, etc. The inventors of the Asserted

Patents understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions from the network, the most exploitable vulnerabilities of most networks are the end-user computers that roam throughout various public and private network domains, potentially exposing those computers to infection and then accessing and potentially infecting the entire and presumably secure computer network.

23. For example, the '705 Patent explains that "[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected network to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in authorized ways and/or by unauthorized person[s]." (*See, e.g.*, Ex. 3 at 1:14–31.)

24. The solution to these problems—as specified and claimed in the Asserted Patents—was an advanced departure from the conventional network access control solutions then in use and was then, as it remains today, patent eligible, highly valuable, novel, and non-obvious technology.

D. K.Mizra's Asserted Patent Claims are Presumed Valid

25. K.Mizra asserts that at least, and without limitation, Claim 19 of the '705 Patent and Claim 17 of the '048 Patent have been directly infringed, either literally or under the doctrine

of equivalents. K.Mizra reserves the right to assert additional claims of the Asserted Patents, including both independent and dependent claims, pursuant to the Court's (and other applicable) rules and procedures and as discovery progresses. These claims are referred to herein as the "Asserted Claims."

26. None of the Asserted Claims are directed to abstract ideas, and each employes inventive concepts and is directed to patent-eligible subject matter. All claims of the Asserted Patents are also presumed to be valid and enforceable against SonicWall and others.

27. Indeed, the Asserted Patents' similar common specification and claims demonstrate that the need satisfied by the inventions of the Asserted Claims was long-felt in the industry and thus unconventional. As one example, the '408 Patent provides that "[u]nwanted and/or malicious network communications, such as spam, phishing, work propagation, etc., hamper productivity and the use and enjoyment of computer and network resources by end users, burden affected networks with unauthorized and/or undesired traffic, and expose recipients to the risk of theft, fraud, etc." (Ex. 4 at 1:22–27.) The Asserted Patents' specification further provides that "[t]herefore, there is a need for an effective way to intercept and take corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server-based filtering software." (*Id.* at 1:46–52.)

28. The specification (including the provisions quoted above), the figures (including those included below), and the text related to the figures further illustrate the complex, tiered network system architecture of the inventions captured by the Asserted Claims. These figures include the following:

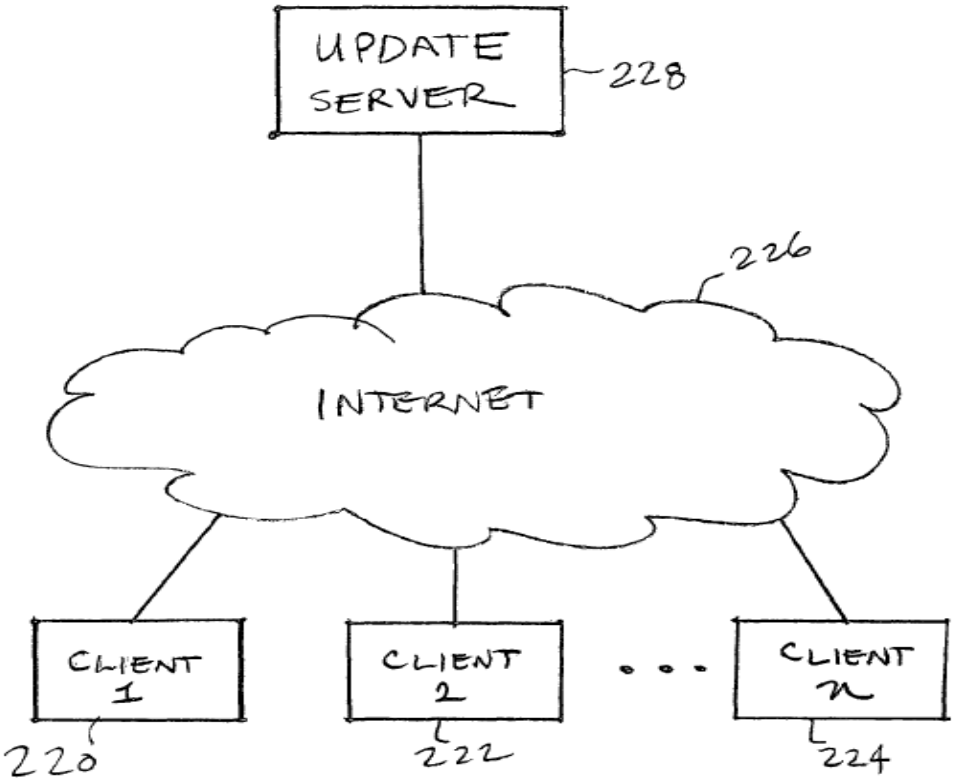
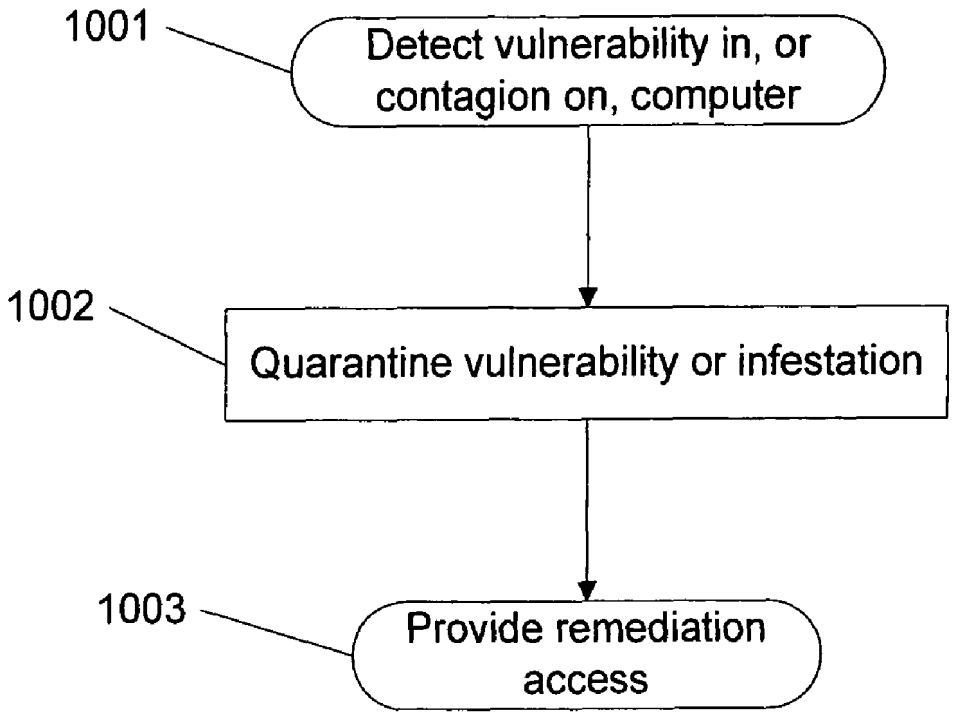


FIG. 2B

(*See* Ex. 3 at Fig. 2B.)



(*See id.* at Fig. 10A.)

29. The foregoing demonstrates that the inventions of the Asserted Claims focus on specific tamperproof hardware that must interact with unique software to improve network access control technology and protect a secure computer network and the data stored thereon from infected devices. As such, the Asserted Claims are eligible as a matter of law for patent protection under step one of *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

30. All actions and steps recited in the Asserted Claims, including the act of quarantining endpoints or other computers, if necessary, requires the involvement of various hardware components running dedicated software both before, during, and after the selection and isolation of an object. Said another way, a claim directed to allowing a machine to automatically and dynamically select and isolate an unsafe device attempting to access a secure network is not simply adding a generic computer component to a fundamentally human process. Rather, it is

removing the once-necessary human intervention from a fundamentally mechanical process, an "improvement in the functioning of a" networked system that simply cannot be considered directed to an abstract concept. *Enfish LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016).

31. As the specification confirms, the improvement captured by the Asserted Claims are not simply quarantining an infected device, but it is instead a multi-faceted network system involving multiple interrelated software and hardware components to protect a network from known and unknown threats. Specifically, the similar specifications of the Asserted Patents disclose that to reduce the burdens of having to manually identify, connect to, isolate, and remove malicious software from an infected device, the networked system can direct an unclean computer attempting to connect to the secure network, known as the host computer, to a form of remediation, such as downloading a software patch or a software update, removing material from the host computer and/or enabling certain settings, etc. present on the host computer. (*See* Ex. 3 at 1:14–41.) Indeed, the inventions of the Asserted Claims are each tethered to these advances over the art in the 2005 time frame, reciting methods and systems that automatically and dynamically detect an insecure condition by contacting a trusted computing base, receiving a response therefrom, determining if that response contains a valid identification of cleanliness, and configuring and implementing a remediation action based on what is discovered about the state of an endpoint or "host" computer. (*See, e.g.,* Ex. 3, Claims 12 and 19; Ex. 4, Claims 10 and 17.) More specifically, the Asserted Claims require a system to communicate with a "trusted computing base" to determine when a response includes a valid digitally signed attestation of cleanliness, and to control access to the network accordingly. These Asserted Claims are thus directed to a machine-implemented solution resolving a machine-specific problem, *i.e.* a machine's difficulty in

detecting, isolating, and remediating infected endpoint devices (*e.g.*, host computers) to prevent contagion of and damage to the larger computer network.

32. The Asserted Claims are thus directed to a machine-implemented process for (1) determining whether the host computer is required to be quarantined, (2) isolating and inoculating the contagions (including directing the host to software programs and/or code designed to identify undesirable and/or unauthorized states) by quarantining the host, (3) limiting access to the network by the host computer so that the unsafe condition thereof can be remedied, and (4) allowing for remediation of an unsafe or infected host computer. As such, the Asserted Claims recite inventions with specific applications or improvements to technologies in the marketplace and cannot be considered abstract or patent ineligible under relevant law.

E. Failed IPRs

33. Fortune 100 companies accused of infringing the Asserted Patents have previously filed petitions for IPRs against each of the Asserted Patents, alleging that the claims of the Asserted Patents should be held invalid as either anticipated or obvious considering art not previously considered. Ultimately, the PTAB instituted an IPR against the ’705 Patent, with similar third party IPRs that were subsequently filed being joined to the first filed and instituted IPR.

34. The PTAB eventually issued its decision holding that no claims of the ’705 Patent were unpatentable, finding that no asserted prior art reference alone or in combination satisfied the limitation of “providing . . . an IP address of a quarantine server configured to serve the quarantine notification page” that was present in all claims of the ’705 Patent.

35. Similarly, petitions for IPR were filed against the ’048 Patent, but the PTAB denied institution of those, stating that the ’048 Patent IPRs were “closely related” to the ’705 Patent IPR petitions, that the petitions were based on and cited the same prior art and that “the challenged

claims [were] materially the same as [those recited in] the '705 patent's claims." The PTAB then offered that it had already "issued a Final Written Decision in [the '705 Patent's IPR], finding no claims of the '705 patent unpatentable" and that the '048 Patent IPRs petition were being denied institution for the same reasons.

36. The '705 Patent IPR Decision was then appealed to the CAFC, which reversed the PTAB's Decision on a few narrow procedural issues involving proof that the asserted prior art references actually would be combined by a person having ordinary skill in the art, as alleged by the petitioners.

37. The parties to the IPRs have moved to dismiss them with prejudice and await issuance of the PTAB's order.

F. SonicWall's Accused Instrumentalities And Services

38. SonicWall has been making, selling, using, and offering for sale computer network security products and services that infringe the Asserted Patents in violation of 35 U.S.C. § 271 (collectively, "the Accused Instrumentalities"). These Accused Instrumentalities include, but are not limited to, SonicWall's Secure Mobile Access (SMA) software and equipment, including the SonicWall appliances (*e.g.*, the SMA 210 Appliance and the SMA 410 Appliance), the sale, offer for sale, use and construction in the United States of which constitutes infringement of at least and without limitation, the Asserted Claims directly, either literally or under DOE.

COUNT I
(Patent Infringement Under 35 U.S.C. § 271 of the '705 Patent)

39. K.Mizra incorporates paragraphs 1 through 38 as though fully set forth herein.

40. The '705 Patent includes 19 claims.

41. SonicWall has directly infringed one or more claims of the '705 Patent by making, importing, using, offering for sale, and/or selling the Accused Instrumentalities, all in violation of 35 U.S.C. § 271(a).

42. Based on publicly available information, the Accused Instrumentalities satisfy every element of at least Claim 19 of the '705 Patent.

43. For example, Claim 19 of the '705 Patent states:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes:
>
> [B1] contacting a trusted computing base associated with a trusted platform module within the first host,
>
> [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
>
> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,

> [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
>
> [F] permitting the first host to communicate with the remediation host.

(Ex. 3 at 22:14-49.)

44. Regarding the preamble of Claim 19, to the extent it is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product for protecting a network." For example, SonicWall touts that its SMA "series products offer complete security for remote access to corporate resources hosted on-prem, in cloud and in hybrid datacenters."

(*See* Ex. 5, Secure Mobile Access (SMA) (available at https://www.sonicwall.com/products/remote-access) (last accessed Jan. 6, 2025).) Additionally, SonicWall SMA products deliver end point (*e.g.*, host computers) posture assessments and ensure

that end points meet security and compliance policies before they are allowed to access a protected network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

(*See* Ex. 6, Secure Mobile Access 1000 Series, p. 2 (SMA 6210, 7210, 8200v) (available at https://www.sonicwall.com/resources/datasheet/secure-mobile-access-1000-series) (last accessed Jan. 6, 2025).) Accordingly, and to the extent the preamble of Claim 19 is somehow limiting, the Accused Instrumentalities would meet the limitation.

45. Limitation A of Claim 19 requires "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The Accused Instrumentalities also meet all the requirements of limitation A of Claim 19. For example, SonicWall's SMA products deliver end point posture assessments and ensure that end points meet security and compliance policies before they connect to the network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

(*See id.*)

About End Point Control

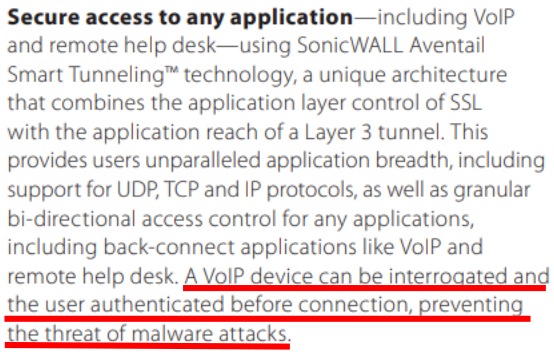
The SMA appliance includes support for End Point Control, which you can use to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments. End Point Control works by:

- Verifying that the user's environment is secure
- Controlling access to sensitive resources

(*See* Ex. 7, Secure Mobile Access 12.4.3 Administration Guide, at 455 (available at https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-admin_guide.pdf) (last accessed Jan. 6, 2025).) Accordingly, the Accused Instrumentalities meet limitation A of Claim 19.

46. Limitation B1 of Claim 19 requires that "detecting [an] insecure condition includes . . . contacting a trusted computing base associated with a trusted platform module within the first host." The Accused Instrumentalities meet these requirements by, for example, the SonicWall SMA product using Connect Tunnel with Smart Tunneling which "enables secure, authorized access to Web based and client/server applications, and file shares." (*See* Ex. 8, Secure Mobile Access 12.4, Connect Tunnel User Guide, p. 4 (available at https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-connect_tunnel_guide.pdf) (last accessed Jan. 6, 2025).) Connect Tunnel obtains information from several sources to determine if

the trusted computing base included as part of the host computer is insecure and it includes a trusted platform module:



Secure access to any application—including VoIP and remote help desk—using SonicWALL Aventail Smart Tunneling™ technology, a unique architecture that combines the application layer control of SSL with the application reach of a Layer 3 tunnel. This provides users unparalleled application breadth, including support for UDP, TCP and IP protocols, as well as granular bi-directional access control for any applications, including back-connect applications like VoIP and remote help desk. A VoIP device can be interrogated and the user authenticated before connection, preventing the threat of malware attacks.

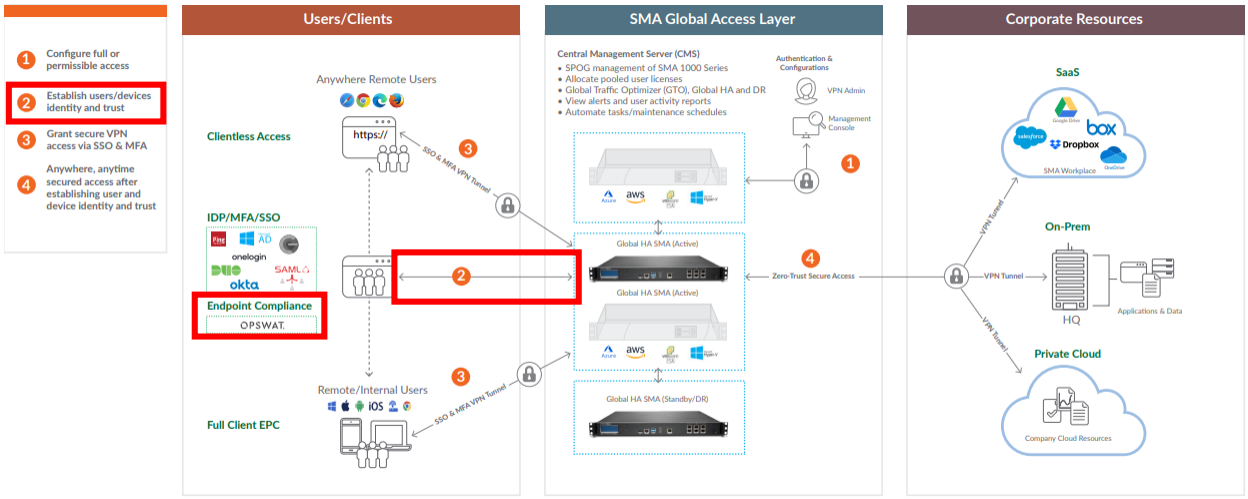
(*See* Ex. 9, SonicWALL Aventail Connect Tunnel, p. 1 (available at https://www.sonicguard.com/datasheets/aventail/Aventail_Connect_Tunnel_DS_US.pdf?srsltid=AfmBOorpvoKAH5lmvKApFNGReBXKszOZGBhPPAy_EooRnAp-tz-sfyk2) (last accessed Jan. 6, 2025).)

```
1. Requirements:

MCT client in 12.2.0 is a Tech Preview release
MCT client can co-exist with CT client
Supported on Windows platforms
Tested and certified on X86 and X64 Win 7 SP1 and Win 10 RS3/RS4
Works on X64 Win 10 clients (build 1607 and later) with following components enabled (CT fails to connect)

-CPU with virtualization extensions (such as VT-x for Intel and AMD-V for AMD processors) enabled
-Trusted Platform Module (TPM 2.0) enabled
-UEFI firmware version 2.3.1.c or higher is used
-UEFI Secure Boot is enabled to ensure that the device boots only authorized code
-Isolated user mode is enabled
-Device gaurd is enabled

2. AMC configuration:

No special configuration required

3. Client configuration:

No special configuration required

4. Known issues:

 ID     Summary
201280  SMA-151: AMC shows MCT user session as Connect Tunnel
203733  SMA-151: MCT caches certificate store and fails to pick from the other
204128  SMA-151: MCT fails to detect outbound proxy
203672  SMA-151: MCT shows setup successful on installation/uninstallation
204614  SMA-151: SMB share access is inconsistent with MCT client
202211  SMA-151: Support basic EPC for file name with attributes size, last modified and integrity check
202126  SMA-151: Support MCT upgrade similar to CT client software upgrade
203670  SMA-151: Suppress the command prompt window during installation and un-installation of MCT

5. Limitations

Works only with SMA 1000 appliance platforms running firmware 11.4.0 and later
Supported only on Windows platforms
Captive portal detection is not supported
Always on VPN is not supported
No support for L10n clients
Custom branding is not supported
Dynamic routing as in CT client is not supported (adding route when resource is accessed)
```

(*See* Ex. 10, SMA1000-151_Modern_CT_Client_for_Windows_Phase1Tunnel (available at https://software.Sonicwall.com/ConnectTunnel/Documentation/SMA1000-151_Modern_CT_Client_for_Windows_Phase1.txt) (last accessed Jan. 6, 2025).) Therefore, the Accused Instrumentalities meet limitation B1 of Claim 19.

47. Limitation B2 requires that "detecting the insecure condition" also includes "receiving a response and determining whether the response includes a valid digitally signed attestation of cleanliness." The Accused Instrumentalities also meet all the requirements of

limitation B2, as the SMA products receive from the host computer requested information and then determines, based on the information received, whether a remote user device (*i.e.*, first host) attempting to access corporate resources (*i.e.*, a protected network) is compliant or trusted by enabling policy-enforced access control and context-aware device authentication. (*See, e.g.*, Ex. 6 at 2.) This process requires back and forth communication between the end point and the SMA products regarding the cleanliness of the device and as the below shows, those communications occur:



(*See* Ex. 11, SonicWall Secure Mobile Access (SMA), at 2 (available at https://www.sonicwall.com/resources/datasheet/datasheet-sonicwall-secure-mobile-access-sma) (last accessed Jan. 6, 2025).) Additionally, SonicWall checks digital signatures from all end points:

Digital Certificates Overview:

A digital certificate is an electronic means to verify identity by a trusted third party known as a **Certificate Authority (CA).** The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs.

Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

(*See* Ex. 12, Digital Certificate Overview (available at https://www.sonicwall.com/support/knowledge-base/digital-certificate-overview/170503430974021) (last accessed Jan. 6, 2025).) Further, these digital signatures are configured to provide information related to the end point.

Data Section:

The data section typically contains information such as,

1. The version of X.509 supported by the certificate
2. A certificate serial number
3. Information about the user's public key
4. The Distinguished Name (DN)
5. Validation period for the certificate
6. Optional information such as the target use of the certificate.

(*See id.*) Thus, the Accused Instrumentalities meet limitation B2 of Claim 19.

48. Limitation C requires that "the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." The Accused Instrumentalities meet these requirements as the SMA products check the compliance of each end point device attempting to connect to the protected network by performing an end point control check that involves matching the end point configuration parameters received from the end point device with specific device profile attributes, such as antimalware programs and applications:

About End Point Control

The SMA appliance includes support for End Point Control, which you can use to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments. End Point Control works by:

- Verifying that the user's environment is secure
- Controlling access to sensitive resources

(*See* Ex. 7, at 455.)

Defining Device Profiles for a Zone

A device profile establishes a trust relationship with a client device by looking for one or more attributes, such as an antimalware program, application, or Windows registry entry. Device profiles can be referenced by one or more zones.

A device profile can be defined to detect only one attribute on a client computer, or it can require multiple attributes. When a device profile references multiple attributes, each of those attributes must be present on a client computer for there to be a match.

ⓘ **NOTE:** For information on how to copy or delete a device profile, see Adding, Editing, Copying, and Deleting Objects in AMC.

(*See id.*)

Digital Certificates Overview:

A digital certificate is an electronic means to verify identity by a trusted third party known as a **Certificate Authority (CA).** The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs.

Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

(*See also* Ex. 12.) Accordingly, the Accused Instrumentalities meet limitation C of Claim 19.

49. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Accused Instrumentalities further meet these requirements by having the SMA products quarantine noncompliant, *i.e.*, unclean, end point devices attempting to connect to the protected network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

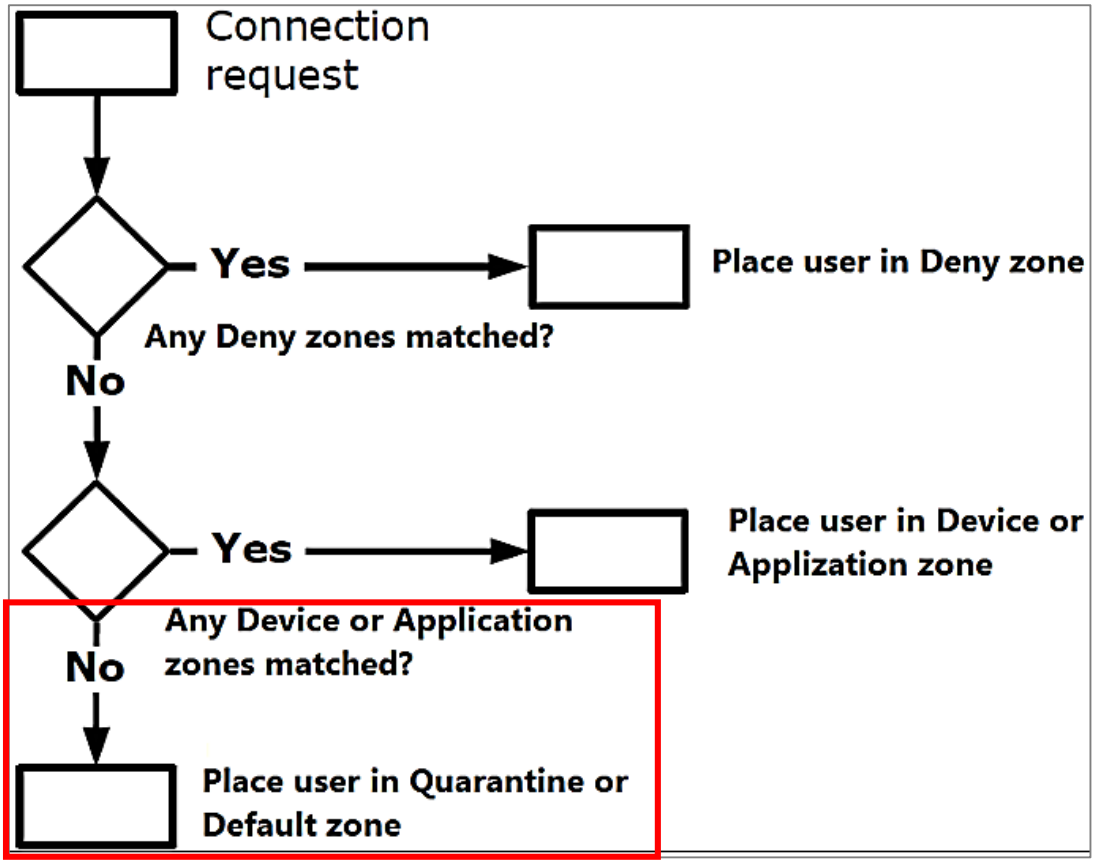
The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

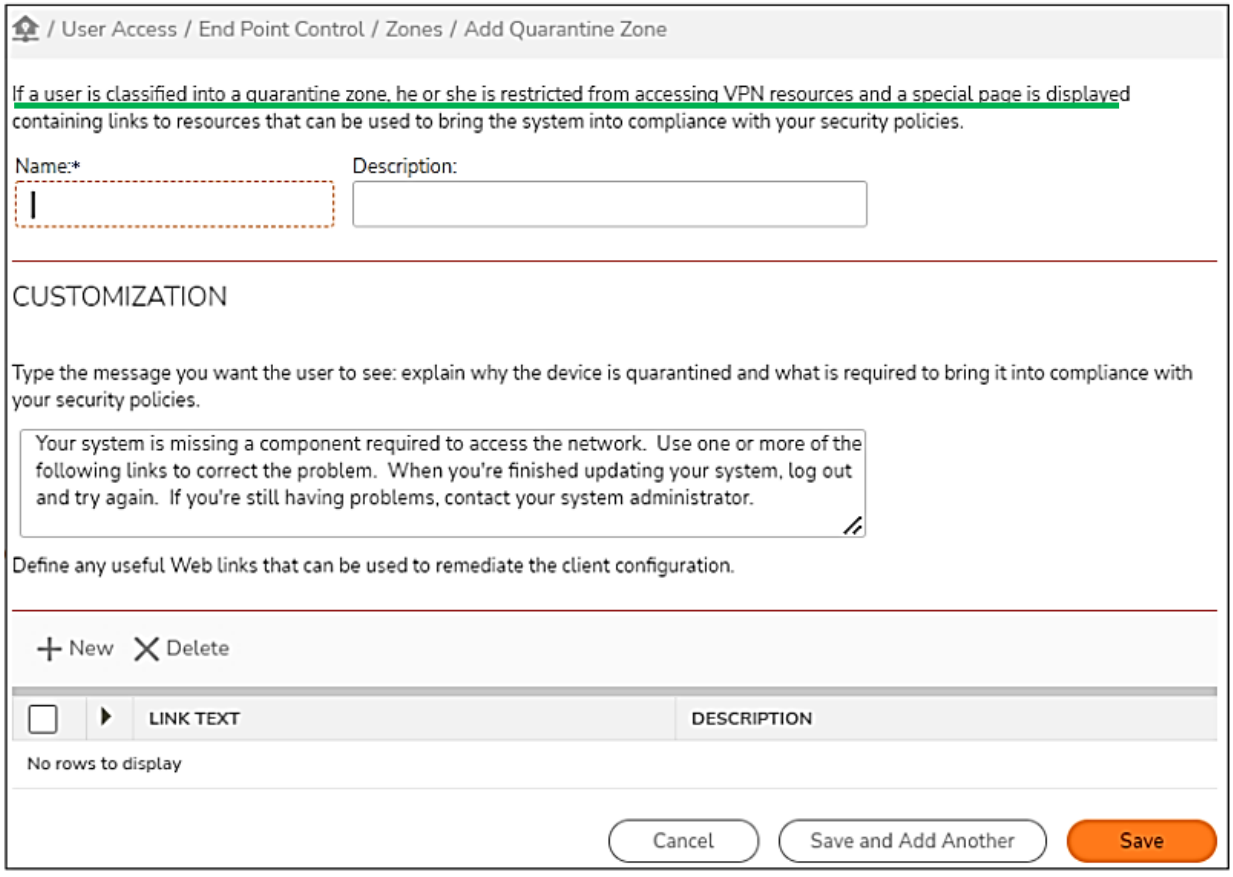
(*See* Ex. 6 at 2.)



(*See* Ex. 7, at 458.) Accordingly, the Accused Instrumentalities meet limitation D of Claim 19.

50. Limitation E1 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes . . . receiving a service request

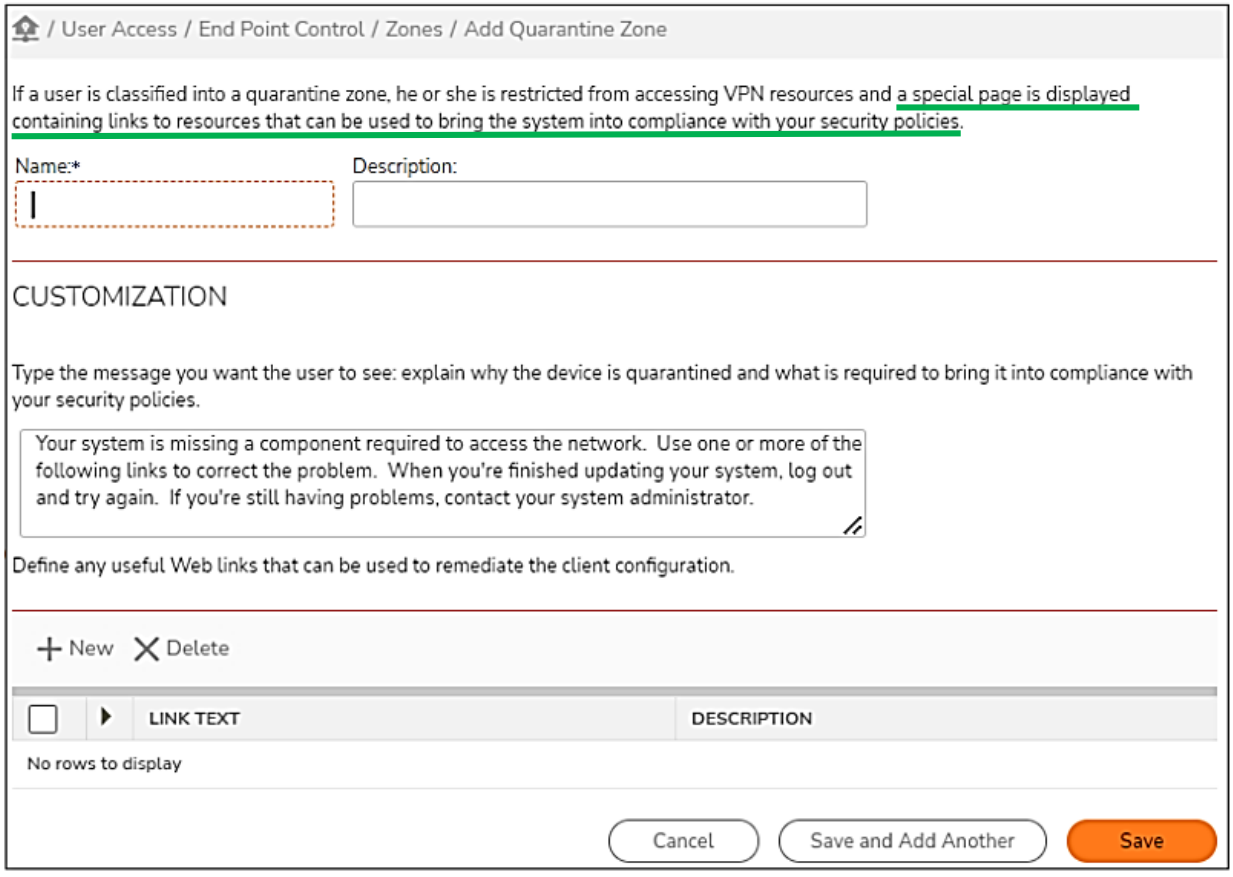
sent by the first host [and] serving a quarantine notification page to the first host when the service request comprises a web server request." The Accused Instrumentalities meet these requirements because the SMA products are configured to determine if an end point device matches the profile designated for such a device and if the end point device does not match, it is placed in a quarantine zone and restricted from accessing the protected network, including VPN resources, preventing the unclean device from communicating with other hosts within the protected network. A quarantine message is also delivered to the unclean end point device, notifying its user of the quarantine.



(*See id.* at 471.) Accordingly, the Accused Instrumentalities meet limitation E1 of Claim 19.

51. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request

comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." The Accused Instrumentalities also meet all the requirements of limitation E2 of Claim 19. For example, SMA provides the user with a quarantine notification page containing links, or IP address(es), with resources (*i.e.* quarantine servers) configured to resolve the quarantine. In other words, SMA provides remediation information to bring the device into compliance so that it can access the protected network.



(*See id.*) Accordingly, the Accused Instrumentalities meet limitation E2 of Claim 19.

52. Limitation F requires "permitting the first host to communicate with the remediation host." The Accused Instrumentalities meet these requirements as the SMA products

allow a quarantined end point device to access web resources to help make the device complaint. (*See id.*) Accordingly, the Accused Instrumentalities meet limitation F of Claim 19.

53. Additionally and/or alternatively, SonicWall has indirectly infringed and continues to indirectly infringe one or more of the claims of the '705 Patent, in violation of 35 U.S.C. § 271(b) by actively inducing users of the SMA system and/or devices operating in the SMA ecosystem to directly infringe one or more claims of the '705 Patent. For example, (a) SonicWall had actual knowledge of or was willfully blind to the existence of the '705 Patent no later than receipt of this Complaint, (b) SonicWall intentionally causes, urges, or encourages users of the accused SMA products to take action that, when taken directly infringe one or more claims of the '705 Patent. SonicWall's encouragement is accomplished by promoting, advertising, and instructing customers and potential customers to use the SMA products and to use of the software and/or devices utilizing the software, including infringing uses thereof, (c) SonicWall knows (or after reading this Complaint should know) that its actions will induce users of the SMA products and ecosystem to directly infringe one or more claims of the '705 Patent, and (d) users thereof directly infringe one or more claims of the '705 Patent. For instance, at a minimum, SonicWall has supplied and continues to supply the SMA software to customers while knowing that installation and use of thereof will infringe one or more claims of the '705 Patent.

54. SonicWall's acts of infringement have occurred within this District and elsewhere throughout the United States.

55. As a result of SonicWall's infringing conduct, K.Mizra has suffered damages. SonicWall is liable to K.Mizra in an amount that adequately compensates K.Mizra for SonicWall's infringement in an amount that is no less than a fully paid-up, lump-sum, reasonable royalty, together with interest and costs as fixed by this Court under 25 U.S.C. § 284.

COUNT II
(Patent Infringement Under 35 U.S.C. § 271 of the '048 Patent)

56. K.Mizra incorporates paragraphs 1 through 55 as though fully set forth herein.

57. The '048 Patent includes 20 claims.

58. SonicWall has directly infringed one or more claims of the '048 Patent by making, importing, using, offering for sale, and/or selling the Accused Instrumentalities, all in violation of 35 U.S.C. § 271(a).

59. Based on publicly available information, the Accused Instrumentalities satisfy every element of at least Claim 17 of the '048 Patent.

60. For example, Claim 17 of the '048 Patent recites the following:

> [preamble] A computer program product, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes
>
> > [B1] contacting a trusted computing base associated with a trusted platform module within the first host,
> >
> > [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, determining whether the service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,
> >
> > [E2] wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and
>
> [F] permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition.

(Ex. 4 at 22:35–23:9.)

61. Regarding the preamble of Claim 17, to the extent it is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product." For example, SonicWall touts that its SMA "series products offer complete security for remote access to corporate resources hosted on-prem, in cloud and in hybrid datacenters."

(*See* Ex. 5.) Additionally, SonicWall SMA products deliver end point (*e.g.*, host computers) posture assessments and ensure that end points meet security and compliance policies before they are allowed to access a protected network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

(*See* Ex. 6, at 2.) Accordingly, and to the extent the preamble of Claim 17 is somehow limiting, the Accused Instrumentalities would meet the limitation.

62. Limitation A requires "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The Accused Instrumentalities also meet all the requirements of limitation A of Claim 17. For example, SonicWall's SMA products

deliver end point posture assessments and ensure that end points meet security and compliance policies before they connect to the network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

(*See id.*)

About End Point Control

The SMA appliance includes support for End Point Control, which you can use to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments. End Point Control works by:

- Verifying that the user's environment is secure
- Controlling access to sensitive resources

(*See* Ex. 7, at 455.) Accordingly, the Accused Instrumentalities meet limitation A of Claim 17.

63. Limitation B1 requires that "detecting [an] insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host. . . . " The Accused Instrumentalities also meet all the requirements of limitation B1 of Claim 17. The Accused Instrumentalities meet these requirements by, for example, the SonicWall SMA product using Connect Tunnel with Smart Tunneling which "enables secure, authorized access to Web based and client/server applications, and file shares." (*See* Ex. 8, at 4.) Connect Tunnel obtains information from several sources to determine if the trusted computing base included as part of the host computer is insecure and it includes a trusted platform module:

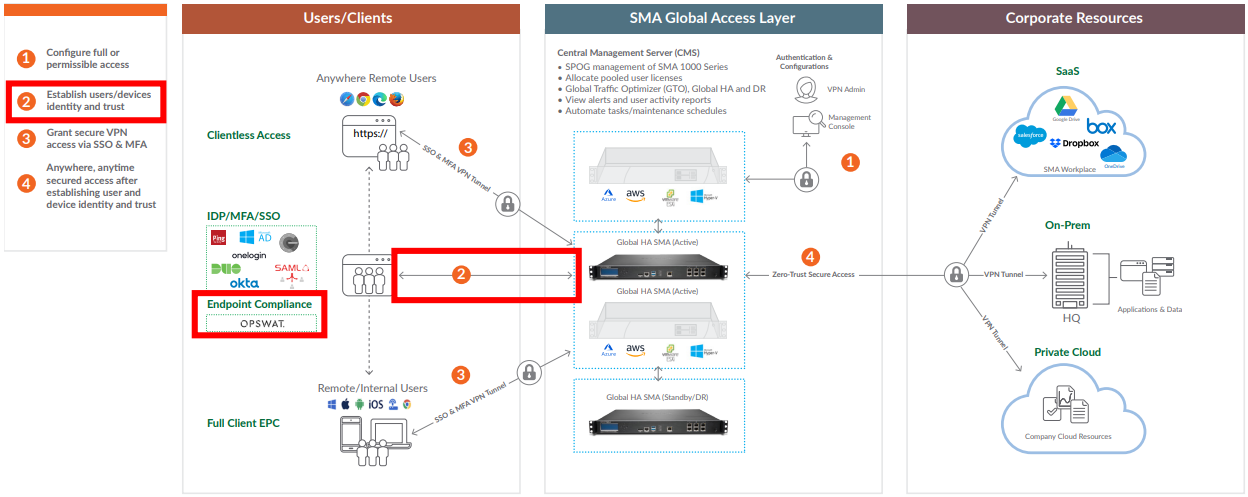
Secure access to any application—including VoIP and remote help desk—using SonicWALL Aventail Smart Tunneling™ technology, a unique architecture that combines the application layer control of SSL with the application reach of a Layer 3 tunnel. This provides users unparalleled application breadth, including support for UDP, TCP and IP protocols, as well as granular bi-directional access control for any applications, including back-connect applications like VoIP and remote help desk. A VoIP device can be interrogated and the user authenticated before connection, preventing the threat of malware attacks.

(*See* Ex. 9, at 1.)

```
1. Requirements:

MCT client in 12.2.0 is a Tech Preview release
MCT client can co-exist with CT client
Supported on Windows platforms
Tested and certified on X86 and X64 Win 7 SP1 and Win 10 RS3/RS4
Works on X64 Win 10 clients (build 1607 and later) with following components enabled (CT fails to connect)

-CPU with virtualization extensions (such as VT-x for Intel and AMD-V for AMD processors) enabled
-Trusted Platform Module (TPM 2.0) enabled
-UEFI firmware version 2.3.1.c or higher is used
-UEFI Secure Boot is enabled to ensure that the device boots only authorized code
-Isolated user mode is enabled
-Device gaurd is enabled

2. AMC configuration:

No special configuration required

3. Client configuration:

No special configuration required

4. Known issues:

 ID     Summary
201280  SMA-151: AMC shows MCT user session as Connect Tunnel
203733  SMA-151: MCT caches certificate store and fails to pick from the other
204128  SMA-151: MCT fails to detect outbound proxy
203672  SMA-151: MCT shows setup successful on installation/uninstallation
204614  SMA-151: SMB share access is inconsistent with MCT client
202211  SMA-151: Support basic EPC for file name with attributes size, last modified and integrity check
202126  SMA-151: Support MCT upgrade similar to CT client software upgrade
203670  SMA-151: Suppress the command prompt window during installation and un-installation of MCT

5. Limitations

Works only with SMA 1000 appliance platforms running firmware 11.4.0 and later
Supported only on Windows platforms
Captive portal detection is not supported
Always on VPN is not supported
No support for L10n clients
Custom branding is not supported
Dynamic routing as in CT client is not supported (adding route when resource is accessed)
```

(*See* Ex. 10.) Therefore, the Accused Instrumentalities meet limitation B1 of Claim 17.

64. Limitation B2 requires that "detecting an insecure condition" also includes "receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness. . . ." The Accused Instrumentalities also meet all the requirements of limitation B2 of Claim 17, as the SMA products receive from the host computer requested information and then determines, based on the information received, whether a remote user device (*i.e.*, first host) attempting to access corporate resources (*i.e.*, a protected network) is compliant or trusted by enabling policy-enforced access control and context-aware device authentication. (*See, e.g.*, Ex. 6 at 2.) This process requires back and forth communication between the end point and the SMA products regarding the cleanliness of the device and as the below shows, those communications occur:



(*See* Ex. 11, at 2.) Additionally, SonicWall checks for digital signatures from all end points:

Digital Certificates Overview:

A digital certificate is an electronic means to verify identity by a trusted third party known as a **Certificate Authority (CA).** The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs.

Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

(*See* Ex. 12.) Further, these digital signatures are configured to provide information related to the end point.

Data Section:

The data section typically contains information such as,

1. The version of X.509 supported by the certificate
2. A certificate serial number
3. Information about the user's public key
4. The Distinguished Name (DN)
5. Validation period for the certificate
6. Optional information such as the target use of the certificate.

(*See id.*) Thus, the Accused Instrumentalities meet limitation B2 of Claim 17.

65. Limitation C requires that "the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." The Accused Instrumentalities also meet all the requirements of limitation C of Claim 17. The Accused Instrumentalities meet these requirements as the SMA products check the compliance of each end point device attempting to connect to the protected network by performing an end point control check that involves matching the end point configuration parameters received from the end point device with specific device profile attributes, such as antimalware programs and applications:

About End Point Control

The SMA appliance includes support for End Point Control, which you can use to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments. End Point Control works by:

- Verifying that the user's environment is secure
- Controlling access to sensitive resources

(*See* Ex. 7, at 455.)

Defining Device Profiles for a Zone

A device profile establishes a trust relationship with a client device by looking for one or more attributes, such as an antimalware program, application, or Windows registry entry. Device profiles can be referenced by one or more zones.

A device profile can be defined to detect only one attribute on a client computer, or it can require multiple attributes. When a device profile references multiple attributes, each of those attributes must be present on a client computer for there to be a match.

ⓘ **NOTE:** For information on how to copy or delete a device profile, see Adding, Editing, Copying, and Deleting Objects in AMC.

(*See id.*)

Digital Certificates Overview:

A digital certificate is an electronic means to verify identity by a trusted third party known as a **Certificate Authority (CA).** The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs.

Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

(*See also* Ex. 12.) Accordingly, the Accused Instrumentalities meet limitation C of Claim 17.

66. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Accused Instrumentalities also meet all the requirements of limitation D of Claim 17. The Accused Instrumentalities further meet these requirements by having the SMA products quarantine noncompliant, *i.e.*, unclean, end point devices attempting to connect to the protected network:

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

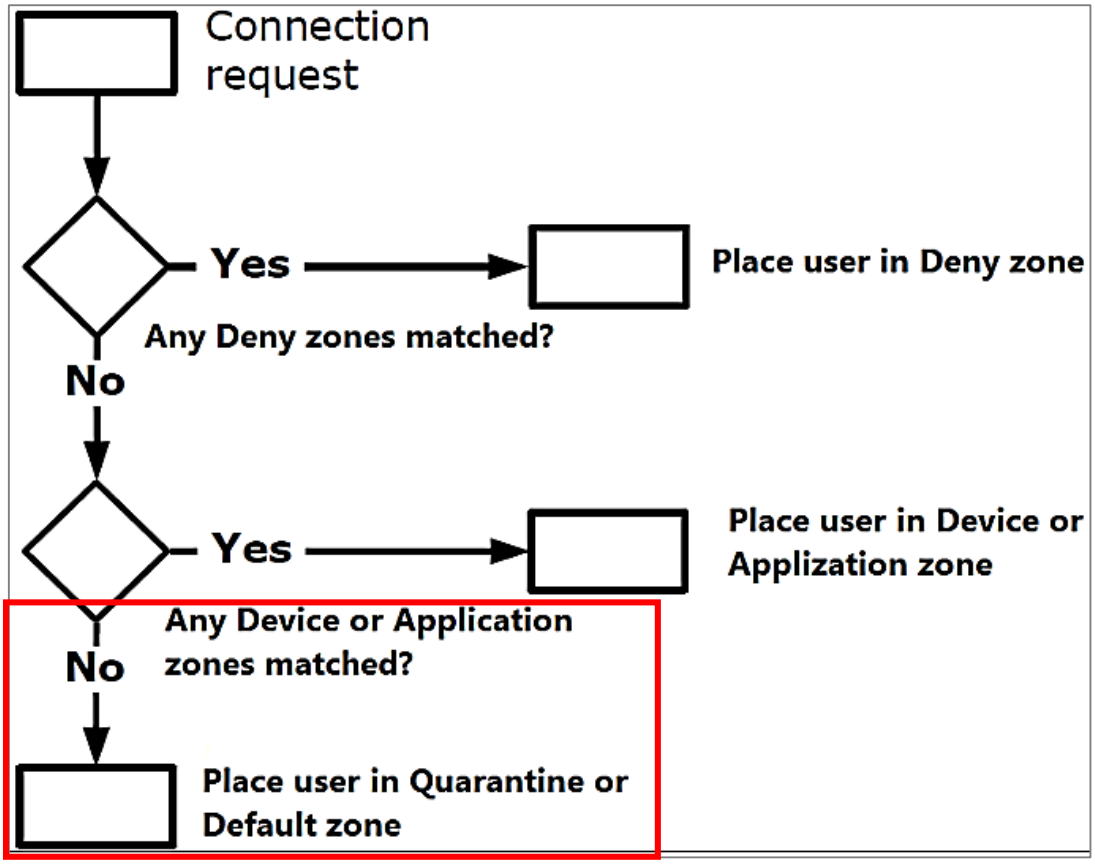
The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

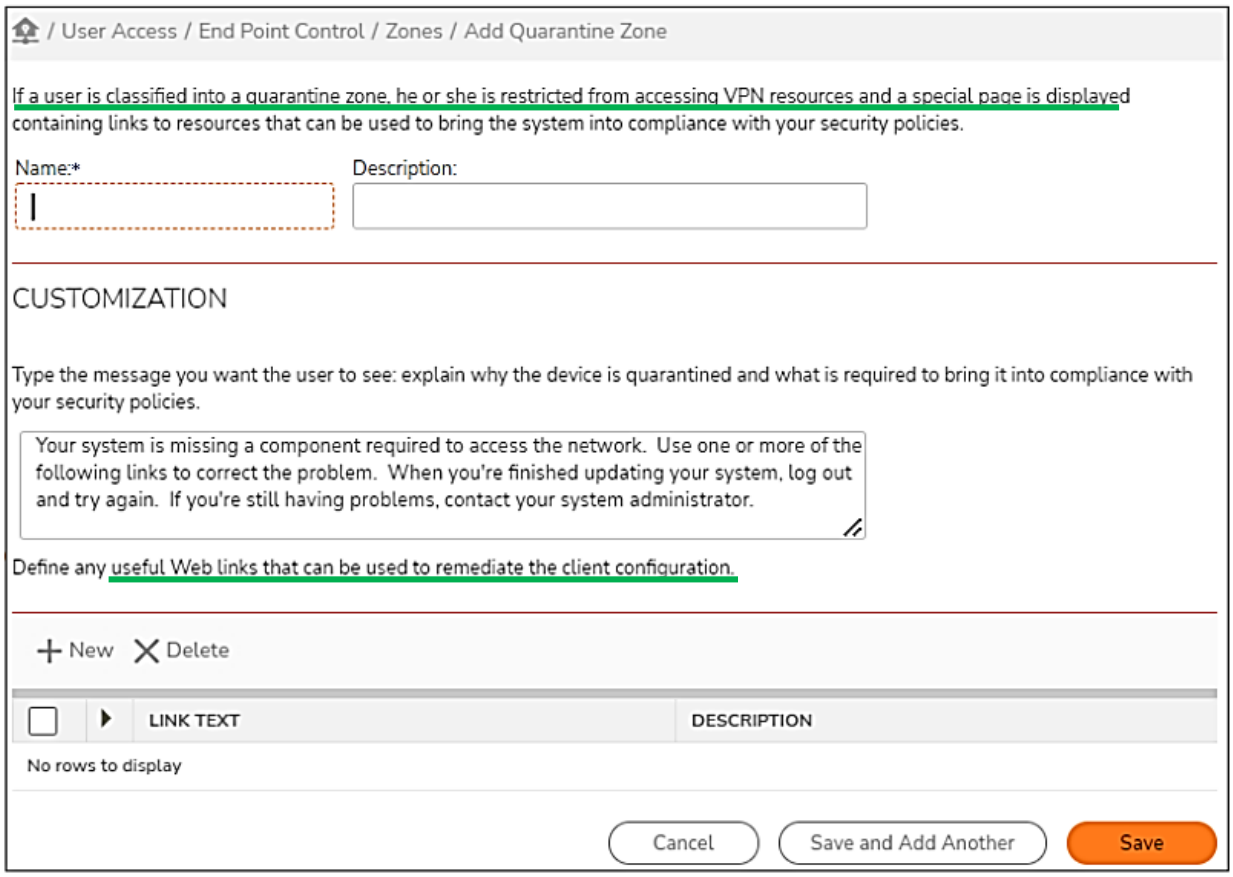
(*See* Ex. 6 at 2.)



(*See* Ex. 7, at 458.) Accordingly, the Accused Instrumentalities meet limitation D of Claim 17.

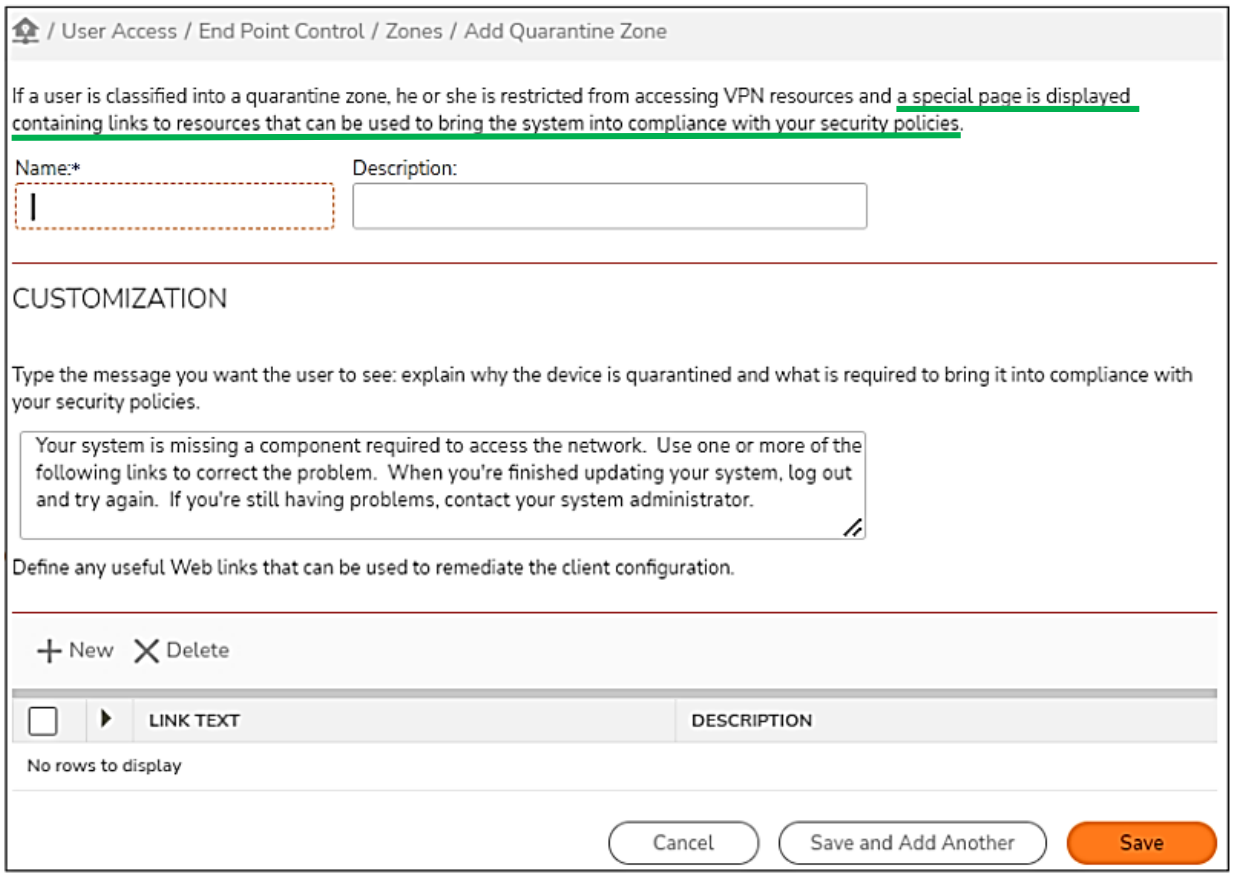
67. Limitation E1 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent

by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request. . . .” The Accused Instrumentalities also meet all the requirements of limitation E1 of Claim 17. The Accused Instrumentalities meet these requirements because the SMA products are configured to determine if an end point device matches the profile designated for such a device and if the end point device does not match, it is placed in a quarantine zone and restricted from accessing the protected network, including VPN resources, preventing the unclean device from communicating with other hosts, including preventing the first end point device from sending data to other hosts, within the protected network. A quarantine message is also delivered to the unclean end point device, notifying its user of the quarantine and providing the user with remediation information to the end point device.



(*See id.* at 471.) Accordingly, the Accused Instrumentalities meet limitation E1 of Claim 17.

68. Limitation E2 requires that "serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page. . . ." The Accused Instrumentalities also meet all the requirements of limitation E2 of Claim 17. For example, SMA provides the user with a quarantine notification page containing links, a method of re-routing the end user to resources (*i.e.* quarantine servers) configured to resolve the quarantine. In other words, SMA re-routs the user using a quarantine server to a page notifying the user of its end point's quarantine.



(*See id.*; *see also id.* at 6 ("This appliance makes applications available from a range of access methods-including a standard Web browser.").) As shown above, the user may be blocked from accessing network resources, in which case SMA re-directs the requesting user's browser to a "special page," that is, a quarantine notification page served by a quarantine server. Accordingly, the Accused Instrumentalities meet limitation E2 of Claim 17.

69. Limitation F requires "permitting the first host to communicate with the remediation host configured to provide data useable to remedy the insecure condition." The Accused Instrumentalities also meet all the requirements of limitation F of Claim 17. The Accused Instrumentalities meet these requirements as the SMA products allow a quarantined end point device to access web resources to help make the device complaint. (*See id.*) Accordingly, the Accused Instrumentalities meet limitation F of Claim 17.

70. Accordingly, the Accused Instrumentalities meet all the limitations of and therefore infringe at least Claim 17 of the ’048 Patent.

71. Additionally and/or alternatively, SonicWall has indirectly infringed and continues to indirectly infringe one or more of the claims of the ’048 Patent, in violation of 35 U.S.C. § 271(b) by actively inducing users of the SMA system and/or devices operating in the SMA ecosystem to directly infringe one or more claims of the ’048 Patent. For example, (a) SonicWall had actual knowledge of or was willfully blind to its existence no later than receipt of this Complaint, (b) SonicWall intentionally causes, urges, or encourages users of the accused SMA products to take action that, when taken directly infringe one or more claims of the ’048 Patent. SonicWall’s encouragement is accomplished by promoting, advertising, and instructing customers and potential customers to use the SMA products and to use the software and/or devices utilizing the software, including infringing uses thereof, and (c) SonicWall knows (or after reading this Complaint should know) that its actions will induce users of the SMA products and ecosystem to directly infringe one or more claims of the ’048 Patent, and (d) users thereof directly infringe one or more claims of the ’048 Patent. For instance, at a minimum, SonicWall has supplied and continues to supply the SMA software to customers while knowing that installation and use of thereof will infringe one or more claims of the ’048 Patent.

72. SonicWall’s acts of infringement have occurred within this District and elsewhere throughout the United States.

73. As a result of SonicWall’s infringing conduct, K.Mizra has suffered damages. SonicWall is liable to K.Mizra in an amount that adequately compensates K.Mizra for SonicWall’s infringement in an amount that is no less than a fully paid-up, lump-sum, reasonable royalty, together with interest and costs as fixed by this Court under 25 U.S.C. § 284.

REQUEST FOR RELIEF

WHEREFORE, K.Mizra respectfully requests the Court find in its favor and against SonicWall, and that the Court grant K.Mizra at least the following relief:

A. Judgment that SonicWall has directly infringed, literally and/or under the DOE, one or more claims of the Asserted Patents;

B. Awarding damages to K.Mizra in an amount to be proven at trial and in the form of a fully paid-up, lump sum, reasonable royalty that takes into account and runs through expiration of the Asserted Patents;

C. Awarding enhanced damages, as appropriate, under 35 U.S.C. § 284;

D. Awarding K.Mizra's costs (including disbursements) and declaring this an exceptional case and awarding K.Mizra its attorneys' fees in accordance with 35 U.S.C. § 285;

E. Pre-judgment and post-judgment interest at the maximum rate permitted by law on the damages caused to K.Mizra by reason of SonicWall's infringing activities and other conduct complaint of herein; and

F. Awarding such other and further relief as this Court deems just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), K.Mizra hereby demands a trial by jury on all issues so triable.

Dated: January 10, 2025

BAYARD, P.A.

/s/ Stephen B. Brauerman
Stephen B. Brauerman (No. 4952)
Ronald P. Golden, III (No. 6254)
600 N. King Street, Suite 400
Wilmington, DE 19801
(302) 655-5000
sbrauerman@bayardlaw.com
rgolden@bayardlaw.com

Attorneys for Plaintiff K.Mizra LLC

OF COUNSEL:

Robert R. Brunelli
Brian S. Boerman
Tristan D. Lewis
SHERIDAN ROSS P.C.
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700
litigation@sheridanross.com
rbrunelli@sheridanross.com
bboerman@sheridanross.com
tlewis@sheridanross.com